An Integrated V&V Environment for Critical Systems Development

Issa Traoré
University of Victoria
Department of Electrical and
Computer Engineering
PO Box 3055 STN CSC
Victoria BC V8W 3P6
Canada
(itraore@ece.uvic.ca)

Abstract

This paper is an introduction to the demonstration sessions for the Precise UML Development Environment (PrUDE). PrUDE is a software V&V platform that integrates in a cost-effective way various rigorous software analysis methodologies.

1. Introduction

Inspite of the current orientation of the software industry where time-to market seems to be the prevalent criteria, higher quality still remains the primary concern of most critical software development projects.

A solution for achieving a high level of confidence in software systems consists of using formal validation and verification (V&V) techniques during their development. Unfortunately, most programs are produced directly from informal requirements without any effective specifications. When specifications are produced before, they are scarcely performed using a formal notation. Because formal methods can be esoteric, hindering wide scale use, we have developed a platform called the Precise UML Development Environment (PrUDE) that combines a formal method (e.g. PVS) with an existing graphical object-oriented notation (e.g. UML) to overcome this barrier [1].

The core notation used in the PrUDE platform is the UML, which provides an underlying methodology for specification and refinement, and a diagramatic notation that contributes to communicativeness and friendliness. In order to provide a ground for rigorous software analysis, we have defined a formal semantics for UML constructs in the PVS Specification Language [2]. PVS offers a very general semantic foundation; it is based on a formal notation with powerful mechanisms for verification and validation, which is highly expressive.

Central to the platform is an integrated tool suite that provides support for consistency-checking, model-checking, proof-checking and testing [1]. Model-checking and proof-checking are based on the PVS toolkit that is run in batch mode. The interface of PrUDE with UML is based on XMI, which provides an explicit interchange format for UML based tools. Since all UML tools export the UML model in XMI format, the platform is independent of any UML tool vendors, making it possible to adapt it easily to existing software development environment. PrUDE's main strength is that users have to deal only with graphical notations that are friendly, easy to learn and easy to use. All the formal notations (related to PVS) are processed invisibly at the back end. Test cases are generated from valid UML specifications. PrUDE provides in its current version an automatic test case generator and a test execution component. The beta version of the tool, appropriate documentation and examples are available in our web-site free for download [3].

References

[1] M. Belaid, I. Traoré, *The Precise UML Development Environment Reference Guide*, Technical Report N0 ECE01-2, Department of Electrical and Computer Engineering, University of Victoria, April 2001.

[2] I. Traoré, *An Outline of PVS Semantics for UML Statechart*, Journal of Universal Computer Science, Springer Pub. Co., Nov. 2000.

[3] Information Security and Object technology Research Group (ISOT): http://www.isot.ece.uvic.ca

Proceedings of the Fifth International Symposium on Requirements Engineering (RE'01)
1090-705X/01 $10.00 © 2001 **IEEE**